Security Functional Requirements Planning for Subscription to Cloud Services (Subscriber Viewpoint)

(Tentative: Based on NIST Reference Architecture – Strawman Model 2.2)

THREAT TAXONOMY DEVELOPMENT APPROACH 1

For each Security Functional Area identified in the strawman model:

- Identify the set of threats applicable to each cloud layer in the reference architecture from a subscriber viewpoint

Limitation: There are no layers for components such as Application, Middleware & Abstracted Resource Component (e.g., VM).

I. Security Functional Area: Authentication & Authorization (1) & Identity Management (4)

Layer: *IaaS*

1. Unauthorized Access to an application deployed by IaaS subscriber
2. Unauthorized Access (Read, Modify) to data repository deployed by IaaS subscriber
3. Unauthorized Access to VM Image Repository (provided by subscriber or provider)
4. Unauthorized creation of VM Images (by cloning from an Image or Running VM instance)
5. Unauthorized creation of VM Snapshots
6. Unauthorized operation on VMs such as start, suspend and stop

Layer: *PaaS*

7. Unauthorized Access to development platforms
8. Unauthorized Access to development tools, deployment libraries
9. Unauthorized Access to an application deployed by PaaS subscriber
10. Unauthorized Access (Read, Modify) to data repository deployed by PaaS subscriber

Layer: SaaS

11. Unauthorized Access to an application provided by SaaS provider
12. Unauthorized Access (Read, Modify) to portion of the application data belonging to a SaaS subscriber
13. Unauthorized Access (Modify) to SaaS application configuration information for a subscriber

II. Security Functional Area: Security Policy Management (7)

II. 1. Sub Area: Application Vulnerability Management

Layer: *IaaS*

1. Presence of Application vulnerabilities such as injection flaws and cross-site scripting in applications hosted by Cloud subscriber.

Layer: *PaaS*

2. Presence of Application vulnerabilities such as injection flaws and cross-site scripting in applications hosted by Cloud subscriber.

II. 2. Sub Area: VM Vulnerability Management

Layer: *IaaS*

3. Presence of insecure VMs (due to lack of latest patches)
4. VMs placed in an insecure state after a re-start (due to patches getting outdated during dormant period)

THREAT TAXONOMY DEVELOPMENT APPROACH 2

1. IGNORE the Security Functional Area for identifying threats (from a subscriber viewpoint) and use it later on for stating security functional requirements.
2. Identify the set of threats applicable to each of the cloud layers – Application, Middleware, Abstract Resource (Computing/Storage etc) (NOT SPECIFIED IN NIST REFERENCE MODEL)

Example

Architecture Component Layer: Abstract Resource (Computing)

1. Unauthorized Access to VM Image Repository (provided by subscriber or provider)
2. Unauthorized creation of VM Images (by cloning from an Image or Running VM instance)
3. Unauthorized creation of VM Snapshots
4. Unauthorized operation on VMs such as start, suspend and stop
5. VM placed in an insecure state after restart
6. VM placed in an insecure state after migration to a new host
7. Side Channel Attack: One VM attacking another
8. A Rogue VM hogs the resources of a hypervisor host denying execution of other VMs
9. Presence of covert channel between VMs

10. A traffic meant for one VM is delivered to a wrong VM or to an entity outside the virtual network.